



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10224763 A**(43) Date of publication of application: **21 . 08 . 98**

(51) Int. Cl.

H04N 7/167
H04L 9/14
(21) Application number: **09023551**(22) Date of filing: **06 . 02 . 97**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**
 (72) Inventor:
YANAGAWA YOSHIFUMI
MATSUMI CHIYOKO
YOSHIDA JUNJI
KOBAYASHI MASAOKI
NAGAOKA YOSHITOMI
(54) CIPHERING DEVICE, DECIPHERING DEVICE AND CIPHERING/ DECIPHERING DEVICE

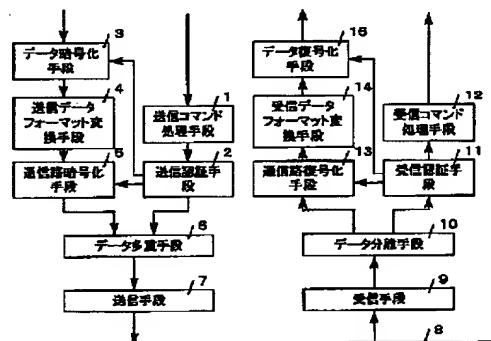
transmitting/receiving data having high secrecy.

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To attain ciphering corresponding to transmitting/receiving data by providing the system with a data ciphering means, a communication line ciphering means, a data deciphering means, and a communication line deciphering means.

SOLUTION: The data ciphering means 3 ciphers AV data consisting of video data and voice data and allowed to be transmitted by a data transmission key received from a transmission certificating means 2 and outputs ciphered transmitting data. The communication line ciphering means 5 ciphers synchronizing transmitting data by a communication transmission key outputted from the means 2 and outputs the ciphered data to a data multiplexing means 6 as ciphered synchronizing transmitting data. On the other hand, the communication line deciphering means 13 receives a communication reception key from a reception certificating means 11, deciphers the ciphered synchronizing receiving data by the communication reception key and generates synchronizing receiving data. The data deciphering means 15 deciphers the ciphered receiving data by a data reception key and generates receiving data. Consequently strong ciphering can be applied only to



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-224763

(43)公開日 平成10年(1998) 8月21日

(51)Int.Cl.⁶

識別記号

F I

H 0 4 N 7/167

H 0 4 N 7/167

H 0 4 L 9/14

H 0 4 L 9/00

6 4 1

審査請求 未請求 請求項の数10 O L (全 14 頁)

(21)出願番号 特願平9-23551

(22)出願日 平成9年(1997) 2月6日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 柳川 良文

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 松見 知代子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 ▲吉▼田 順二

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 滝本 智之 (外1名)

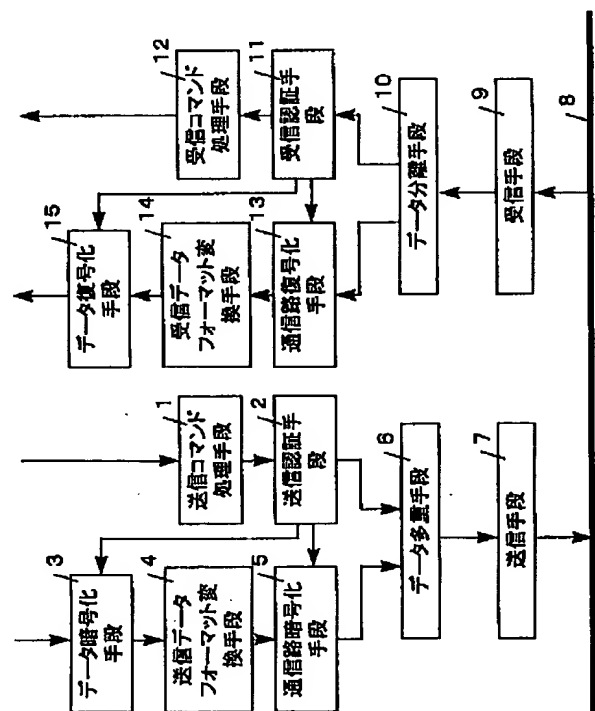
最終頁に続く

(54)【発明の名称】 暗号化装置および復号化装置および暗号化復号化装置

(57)【要約】

【課題】 送受信データの種類や内容により暗号化の強度を変更可能にし、映像の種類や映像データの圧縮形式等に対して柔軟に暗号化を変更可能にする。

【解決手段】 データ用送信キーで送信データを暗号化するデータ暗号化手段3と、データ暗号化手段3の出力の暗号化送信データを同期送信データに変換する送信データフォーマット変換手段4と、通信用送信キーで同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段5と、通信用受信キーで暗号化同期受信データを復号する通信路復号化手段13と、通信路復号化手段13の出力を変換して暗号化受信データを生成する受信データフォーマット変換手段14と、データ用受信キーを用いて暗号化受信データの復号を行い受信データを生成するデータ復号化手段15とを備え、通信路8の暗号化とは独立して、送受信データの種類や内容に応じてデータの暗号化強度を任意に設定する。



【特許請求の範囲】

【請求項1】 送信制御信号を処理する送信コマンド処理手段と、
 前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
 前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、
 前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、
 前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
 前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
 前記データ多重手段の出力する通信用データを通信路上に送出する送信手段と、
 前記通信路から通信用データを受信する受信手段と、
 前記通信用データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
 前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
 前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
 前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
 前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、
 前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを備える暗号化復号化装置。

【請求項2】 送信制御信号を処理する送信コマンド処理手段と、
 前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
 前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、
 前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、
 前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
 前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
 前記データ多重手段の出力する通信用送信データを通信路上に送出する送信手段とを備える暗号化装置。

【請求項3】 通信路から通信用受信データを受信する受信手段と、

前記通信用受信データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
 前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
 前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
 前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
 前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、
 前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを備える復号化装置。

【請求項4】 送信制御信号を処理する送信コマンド処理手段と、
 前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
 前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、
 前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、
 前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
 前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
 前記データ多重手段の出力する通信用データを通信路上に送出する送信手段と、
 前記通信路から通信用データを受信する受信手段と、
 前記通信用データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
 前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
 前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
 前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
 前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、
 前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを備える暗号化復号化装置。

【請求項5】 送信制御信号を処理する送信コマンド処理手段と、
 前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
 前記送信認証手段が出力するデータ用送信キーを用いて

送信データを暗号化する複数のデータ暗号化手段と、
前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、
前記送信認証手段が出力する通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
前記データ多重手段の出力する通信用送信データを通信路上に送出する送信手段とを備える暗号化装置。

【請求項 6】 通信路から通信用受信データを受信する受信手段と、
前記通信用受信データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、
前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを備える復号化装置。

【請求項 7】 受信データ及び送信データは、映像データ及び音声データからなる A V データであることを特徴とする請求項 1 ないし 6 のいずれかに記載の暗号化装置および復号化装置および暗号化復号化装置。

【請求項 8】 映像データはプログレッシブ映像データであることを特徴とする請求項 7 記載の暗号化装置および復号化装置および暗号化復号化装置。

【請求項 9】 送信データフォーマット変換手段は、送信認証手段が出力するデータ用受信キー及びデータ暗号化手段が出力する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換することを特徴とする請求項 1、2、4 または 5 のいずれかに記載の暗号化装置および暗号化復号化装置。

【請求項 1 0】 受信データフォーマット変換手段は、通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データ及びデータ用受信キーを生成し、
データ復号手段は、前記受信データフォーマット変換手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行うことを特徴とする請求項 1、3、4 または 6 のいずれかに記載の復号化装置および暗号化復号化装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、映像機器やオーディオ機器をネットワーク上に接続し、映像及び音声データをネットワークを経由して伝送するネットワークインターフェース装置に関し、特に、ネットワーク上に流す映像及び音声データを変換加工して暗号化するとともに、ネットワーク上から受け取ったデータを変換加工して映像及び音声データに復号化する暗号化装置および復号化装置および暗号化復号化装置に関するものである。

【0 0 0 2】

【従来の技術】近年、ケーブルテレビジョンや通信衛星を用いて、映像データ及び音声データを配信するサービスが開始されており、これらを受信するためのセットトップボックスや家庭用デジタルビデオカメラ等の A V 機器にもネットワークインターフェースをもつ機器が普及してきている。これらの機器をネットワークで接続する際、著作権や課金等の問題により、映像及び音声データに対する暗号化復号化装置が必要とされてきている。

【0 0 0 3】従来、暗号化復号化装置として、例えば特開平 6 - 1 2 5 5 5 4 号公報に記載されているものがあり、暗号化復号化装置に用いられるいくつかの技術を開示している。以下に図面を参照しながら、従来の暗号化復号化装置の一例について説明する。

【0 0 0 4】図 8 は従来の暗号化復号化装置の一例を示すものである。図 8 において、1 は送信コマンド処理手段、2 は送信認証手段、4 は送信データフォーマット変換手段、5 は通信路暗号化手段、6 はデータ多重手段、7 は送信手段、8 は通信路、9 は受信手段、1 0 はデータ分離手段、1 1 は受信認証手段、1 2 は受信コマンド処理手段、1 3 は通信路復号化手段、1 4 は受信データフォーマット変換手段である。

【0 0 0 5】ここで、ネットワーク上へ送信する場合、送信コマンド処理手段 1 は送信先名や機器制御コマンド等からなるコマンド入力を受け、このコマンド入力を送信相手に理解できる制御情報に変換するとともに、送信認証手段 2 に対して送信データの認証及び通信路の認証を要求する。送信認証手段 2 は、例えば、本装置内に記憶させている送信先の公開キーを通信用送信キーとして通信路暗号化手段 5 へ出力するとともに、送信コマンド処理手段 1 から受け取った制御情報を非同期送信データとしてデータ多重手段 6 へ出力する。

【0 0 0 6】一方、映像データや音声データ等からなる送信データは、送信データフォーマット変換手段 4 で通信路 8 のデータフォーマットの同期送信データに変換され、通信路暗号化手段 5 へ出力される。通信路暗号化手段 5 ではこの同期送信データを通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段 6 へ出力する。

【0 0 0 7】データ多重手段 6 は非同期送信データ及び暗号化同期送信データを時分割等の手段で多重化し、送

信手段7はこのデータを通信路8へ送信する。データをネットワーク上から受信する場合、受信手段9は通信路8よりデータを受信し、データ分離手段10で時分割多重されたデータを分離し、暗号化同期受信データ及び非同期受信データを生成する。

【0008】受信認証手段11は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段13へ出力する。ここで、受信された制御情報は受信コマンド処理手段12で処理され、本装置内部で有効なコマンドを生成する。一方、通信路復号化手段13は受信認証手段11から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。受信データフォーマット変換手段14は同期受信データのフォーマット変換を行い、受信データを生成する。

【0009】このようにして、ネットワーク上にある送信先以外の機器に対しては、送信情報を隠匿する。

【0010】

【発明が解決しようとする課題】しかしながら上記のような構成では、通信路の暗号化手法により暗号化の強度が決まってしまう、送受信するデータの内容によって暗号化の強度を変えることができないという問題点を有していた。本発明は上記問題点を解決するもので、送受信データにより暗号化の強度を変更可能にし、送受信データとして用いる映像データの種類、内容や圧縮形式等に対して柔軟に暗号化方法を変更できる暗号化復号化装置を提供することを目的とする。

【0011】

【課題を解決するための手段】上記問題点を解決するために本発明の暗号化復号化装置は、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを具備することを特徴とするものである。

【0012】また、データ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、各々のデータ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送

信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを具備することを特徴とするものである。

【0013】そして、送信データ及び受信データは映像データ又は音声データ等からなるAVデータであることを特徴とするものである。さらに、映像データをノンインターレース方式のプログレッシブ画像データとすることを特徴とするものである。また、データ用受信キーは暗号化送信データ及び暗号化受信データの一部として送受信することを特徴とするものである。

【0014】

【発明の実施の形態】以下、本発明の実施の形態による暗号化復号化装置について、図面を参照しながら説明する。

（実施の形態1）図1は本発明の実施の形態1における暗号化復号化装置のブロック図を示すものである。ここで、従来例と同一の構成要素には同一の符号を付し説明を省略する。

【0015】図1において、1は送信コマンド処理手段、2は送信認証手段、3はデータ暗号化手段、4は送信データフォーマット変換手段、5は通信路暗号化手段、6はデータ多重手段、7は送信手段、8は通信路、9は受信手段、10はデータ分離手段、11は受信認証手段、12は受信コマンド処理手段、13は通信路復号化手段、14は受信データフォーマット変換手段、15はデータ復号化手段である。

【0016】ここで、ネットワーク上へ送信する場合、送信コマンド処理手段1は送信先名や機器制御コマンド等からなるコマンド入力を受け、このコマンド入力を送信相手に理解できる制御情報に変換するとともに、送信認証手段2に対して送信データの認証及び通信路の認証を要求する。この機器制御コマンドは、例えば本装置をVTRやレーザーディスクに組み込むのであれば再生、サーチ等の制御情報であり、これらの情報を受信機器との間で規定したコードに変換し、送信認証手段2へ出力する。

【0017】送信認証手段2は、例えば、本装置内に記憶されている送信先の公開キーを通信用送信キーとして通信路暗号化手段5へ、また、送信データ用の公開キーをデータ用送信キーとしてデータ暗号化手段3へ出力するとともに、送信コマンド処理手段1から受け取った制御情報を非同期送信データとしてデータ多重手段6へ出力する。ここで、必ずしも送信データ用の公開キーや送信先の公開キーをデータ用送信キーや通信用送信キーとして用いる必要はなく、映像等の送信データを送信する

前に送信認証手段2において、非同期データを送受信することにより送信先から暗号化キーを取得しても良いし、本装置に記憶してある秘密キーや乱数により生成した秘密キーを暗号化キーとして用いて暗号化し、この秘密キーに対する公開キーを送信先にのみ非同期データとして送信しても良い。

【0018】さらに、送信先の複数の機器に共通のキーを設定し、このキーの公開キーまたは秘密キーのいずれかをを用いて暗号化しても良い。また、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いてもよい。さらに、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いても良い。さらに、データ用送信キー及びデータ用受信キーは地上波TV放送、CATV、デジタルTV放送、デジタル衛星放送や電話回線等の通信回線を通して受け取ったものとしてもよく、例えば、TV放送等からVTR等に録画したAVデータに対して、VTR等で再生する際に、TV放送等からVTR録画時又はVTR再生時に受け取ったデータ用送信キーで暗号化し、通信路上にある表示機器では装着されているスマートカードに記憶されているデータ用受信キーや電話回線を通して受け取ったデータ用受信キーで復号するとしても良い。

【0019】ここでは、秘密キーと公開キーによる暗号化で説明したが、暗号化復号化を一つのキーで行っても良い。一方、データ暗号化手段3は映像データや音声データからなる送信すべきAVデータ（送信データ）を送信認証手段2から受け取ったデータ用送信キーで暗号化し、暗号化送信データを生成する。

【0020】次に、送信データフォーマット変換手段4は暗号化送信データを通信路のデータフォーマット形式の同期送信データに変換し、通信路暗号化手段5へ出力する。ここで、送信データは、例えばデジタルVTRで使用されているDVデータ形式やMPEGデータ形式のものであり、同期送信データは、例えばIEEE1394-1995で規定されたアイソクロナスパケットの形式のものである。

【0021】通信路暗号化手段5ではこの同期送信データを、送信認証手段2が出力する通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段6へ出力する。データ多重手段6は、例えばIEEE1394-1995に規定された方法を用いて、非同期送信データはアシンクロナスパケットとして、暗号化同期送信データはアイソクロナスパケットとして多重化する。もちろん、ここで、非同期データの転送レートが十分にあれば、時分割多重等の方法で多重化し非同期パケットとして送信しても良い。

【0022】送信手段7は通信路8のバスアービトレーションを行い、バスの使用权を獲得し、アシンクロナス

パケットを送信先に転送するとともに、アイソクロナスパケットに対しては、例えばIEEE1394-1995プロトコルに則り、ある時間周期で周期的に送信先へ送信する。次に、ネットワーク上からデータを受信する場合、受信手段9は通信路8より、例えば、自分宛のアシンクロナスパケット及びアイソクロナスパケットを受信し、データ分離手段10において多重化されたデータを分離し、アシンクロナスパケットから非同期受信データを、アイソクロナスパケットから暗号化同期受信データを取得する。

【0023】受信認証手段11は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段13へ、受信データ用の秘密キーをデータ用受信キーとしてデータ復号化手段15へ出力する。さらに、受信された制御情報は受信コマンド処理手段12で処理され、本装置内部で有効なコマンドを生成する。ここで、通信用受信キー及びデータ用受信キーは必ずしも秘密キーである必要はなく、送信認証手段2の説明で述べたのと同様な方法を用いることが可能である。

【0024】一方、通信路復号化手段13は受信認証手段11から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。受信データフォーマット変換手段14は同期受信データのフォーマット変換を行い、暗号化受信データを生成する。ここで、同期送信データは、例えばIEEE1394-1995で規定されたアイソクロナスパケットの形式のものであり、暗号化受信データは、例えばデジタルVTRで使用されているDVデータ形式のデータを暗号化したものである。

【0025】データ復号化手段15は、暗号化受信データをデータ用受信キーで復号し、受信データを生成する。この受信データは、例えばデジタルVTRで使用されているDVデータである。よって、データ復号化手段15の出力信号を所望の時間間隔でDVエンコード等に入力することにより、NTSC映像データを得られ、例えばTV画面上に表示することが可能となる。ここで、映像データはNTSC映像データとしたが、ノンインターレース方式のプログレッシブ画像データとしてもよく、この時パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現できる。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【0026】以上のように本実施の形態のよれば、データ暗号化手段、通信路暗号化手段、データ復号化手段及

10

20

30

40

50

び通信路復号化手段を用いることにより、送受信データに応じた暗号化を行うことができ、隠匿性の高い送受信データに対してのみ強い暗号化を行うことが容易に実現可能になり、送受信データの内容に応じて柔軟に暗号化強度を変更することが可能になる。

【0027】また、送受信データとして、映像データや音声データからなるAVデータを用いることにより、ペーパービューの映像に対しては見にくいが何の映像であるかは大体理解できるような暗号化を行うことや秘密性の高い映像に対しては強力な暗号化を行うことが可能となり、映像や音声等の内容に応じて暗号化強度を変更できる。

【0028】さらに、TV放送等からVTR等に録画したAVデータに対して、VTR等で再生する際に暗号化することが可能になり、通信路上に接続された表示機器でこのAVデータを視聴することに対して著作権の保護や課金等を行うことができる。なお、本実施の形態においてデータ暗号化手段等からなるデータ送信部とデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、データ用送信キー及びデータ用受信キーをあらかじめ設定しておけば、例えば、映像の再生専用機器においては送信コマンド処理手段、送信認証手段、データ暗号化手段、送信データフォーマット変換手段、通信路暗号化手段、データ多重化手段、送信手段からなるデータ送信部のみを内蔵すればよく、また、モニタのように映像データの受信のみを行う機器では受信コマンド処理手段、受信認証手段、データ復号化手段、受信データフォーマット変換手段、通信路復号化手段、データ分離化手段、受信手段からなるデータ受信部のみを内蔵すればよい。

【0029】また、本実施の形態では送信データ及び受信データは映像データや音声データからなるAVデータであるとしたが、秘密性のある各種データ（例えば、文書データや表データ）に対しても適用可能であり、同様の効果が得られる。そして、本実施の形態で示した各手段は送信手段及び受信手段の通信路ドライブ回路等を除きソフトウェアで実現しても同様の効果が得られる。

【0030】さらに、データ多重手段及び送信手段は一つの手段で構成しても良く、同様の効果が得られる。これはデータ分離手段及び受信手段に関しても同様である。図2は本実施の形態において、送信コマンド処理手段1と受信コマンド処理手段12を送受信コマンド処理手段16で、送信認証手段2と受信認証手段11を送受信コマンド処理手段17で実現した場合のブロック図である。このように構成することにより、送信側と受信側で非同期データをやり取りし、データの送受信、特に非同期データの送受信に必要な認証や機器制御等を行うことが容易になり、種々の機器が通信路8上につながる場合にも柔軟に対応できる。例えば、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、この

キーをデータ用送信キーとして用いて暗号化することや、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いて暗号化することも容易になる。

【0031】ここではデータ暗号化手段等からなるデータ送信部とデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、例えば、映像の再生専用機器においては図3に示すように、送受信コマンド処理手段16、送受信認証手段17、データ暗号化手段3、送信データフォーマット変換手段4、通信路暗号化手段5、データ多重化手段6、送信手段7からなるデータ送信部と送受信認証手段17に接続された非同期データ用の受信手段9のみを用いて暗号化装置を構成すればよい。

【0032】また、モニタのように映像データの受信のみを行う機器では図4に示すように送受信コマンド処理手段16、送受信認証手段17、データ復号化手段15、受信データフォーマット変換手段14、通信路復号化手段13、データ分離化手段10、受信手段9からなるデータ受信部と送受信認証手段17に接続された非同期データ用の送信手段7のみを用いて復号化装置のみを構成すればよい。

【0033】図5は本実施の形態において、データ用送信キーを同期送信データとともに送信し、データ用受信キーを同期受信データとともに受信する場合の例である。ここで、まず、送信認証手段2は、例えば、本装置内に記憶されている送信先の公開キーを通信路暗号化手段5へ、また、送信データ用の公開キーをデータ用送信キーとしてデータ暗号化手段3へ出力するとともに、送信データ用の秘密キーをデータ用受信キーとして送信データフォーマット変換手段4へ出力する。ここで、必ずしも送信データ用の公開キーや秘密キーをデータ用送信キーやデータ用受信キーとして用いる必要はなく、本装置に記憶してある秘密キーや乱数により生成した秘密キーをデータ用送信キーとして用いて暗号化し、この秘密キーに対する公開キーをデータ用受信キーとして用いても良い。さらに、送信先の複数の機器に共通のキーを設定し、このキーの公開キーと秘密キーをデータ用送信キー及びデータ用受信キーとして用いても良い。また、ここでは秘密キーと公開キーによる暗号化で説明したが、暗号化／復号化を一つのキーで行っても良く、この時、データ暗号化手段3及び送信データフォーマット変換手段4へ出力するキーは同一のものとなる。このように構成することにより、データ用受信キーの取り扱いが容易になり、通信路の秘密性を確保しつつ送受信データに対して適切な暗号化を簡単な構成で実現できる。

【0034】次に、送信データフォーマット変換手段4はデータ暗号化手段3の出力する暗号化送信データ及び

データ用受信キーを通信路のデータフォーマット形式の同期送信データに変換し、通信路暗号化手段 5 へ出力する。一方、受信データフォーマット変換手段 1 4 は同期受信データのフォーマット変換を行い、暗号化受信データ及びデータ用受信キーを抽出する。このデータ用受信キーを用いて、データ復号化手段 1 5 は暗号化受信データを復号し、受信データを生成する。このように構成することで、データ用受信キーをあらかじめ受信側の装置内に保持する必要なくなり、構成を簡単化できるとともに、通信路の安全は通信路の暗号化により確保することが可能である。

【0035】（実施の形態 2）以下本発明の実施の形態 2 について図面を参照しながら説明する。図 6、図 7 は本発明の実施の形態 2 を示す暗号化復号化装置のブロック図である。ここで、実施の形態 1 と同一の構成要素には同一の符号を付し説明を省略する。図 6 において、20 は第 1 のデータ暗号化手段、21 は第 1 の送信データフォーマット変換手段、22 は第 N のデータ暗号化手段、23 は第 N の送信データフォーマット変換手段、30 は第 1 のデータ復号化手段、31 は第 1 の受信データフォーマット変換手段、32 は第 N のデータ復号化手段、33 は第 N の受信データフォーマット変換手段である。但し、ここで、N は自然数であり、N 個のデータ暗号化手段及び送信データフォーマット変換手段があることを示している。本実施の形態では第 1 のデータ暗号化手段と第 N のデータ暗号化手段等の 2 つを用いた場合で説明しているが、任意の自然数 N 個のデータ暗号化手段等を用いた場合も本実施の形態と同様の手法で実現可能である。

【0036】まず、ネットワーク上へ送信する場合、送信認証手段 2 は、例えば、本装置内に記憶されている送信先の公開キーを通信用送信キーとして通信路暗号化手段 5 へ、また、第 1 のストリームデータ用の公開キーを第 1 のデータ用送信キーとして第 1 のデータ暗号化手段 20 へ、第 N の送信データ用の公開キーを第 N のデータ用送信キーとして第 N のデータ暗号化手段 22 へ出力するとともに、送信コマンド処理手段 1 から受け取った制御情報を非同期送信データとしてデータ多重手段 6 へ出力する。

【0037】なお、第 1 のデータ用送信キーと第 N のデータ用送信キーとは異なってもよいし同一でもよい。ここで、実施の形態 1 と同様に、必ずしも送信データ用の公開キーや送信先の公開キーをデータ用送信キーや通信用送信キーとして用いる必要はなく、映像等の送信データを送信する前に送信認証手段 2 において、非同期データを送受信することにより送信先から暗号化キーを取得してもよいし、本装置に記憶してある秘密キーや乱数により生成した秘密キーを暗号化キーとして用いて暗号化し、この秘密キーに対する公開キーを送信先にのみ非同期データとして送信してもよい。さらに、送信先

の複数の機器に共通のキーを設定し、このキーの公開キーを用いて暗号化してもよい。

【0038】また、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いてもよい。さらに、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いてもよい。さらに、データ用送信キー及びデータ用受信キーは地上波 TV 放送、CATV、ディジタル TV 放送、ディジタル衛星放送や電話回線等の通信回線を通して受け取ったものとしてもよく、例えば、TV 放送等から VTR 等に録画した AV データに対して、VTR 等で再生する際に、TV 放送等から VTR 録画時又は VTR 再生時に受け取ったデータ用送信キーで暗号化し、通信路上にある表示機器では装着されているスマートカードに記憶されているデータ用受信キーや電話回線を通して受け取ったデータ用受信キーで復号するとしてもよい。

【0039】ここでは、秘密キーと公開キーによる暗号化で説明したが、暗号化復号化を一つのキーで行ってもよい。一方、第 1 のデータ暗号化手段 20 及び第 N のデータ暗号化手段 22 は映像データや音声データからなる送信すべき送信データを送信認証手段 2 から受け取ったデータ用送信キーで暗号化し、暗号化送信データを生成する。ここで、第 1 のデータ暗号化手段 20 には第 1 の送信データが入力され、第 N のデータ暗号化手段 22 には第 N の送信データが入力される。例えば、第 1 の送信データはディジタル VTR で使用されている DV データであり、第 N の送信データはディジタル衛星放送等で使用されている MPEG データであるとする。この時、第 1 のデータ暗号化手段 20 では、第 1 のデータ用送信キーですべてのフレームを同じ暗号化方式で暗号化し、第 N のデータ暗号化手段 22 では、第 N のデータ用送信キーで MPEG データ中の I フレームのみに対して暗号化する。ここで、もちろん、第 1 のデータ暗号化手段 20 と第 N のデータ暗号化手段 22 で同一の暗号化をしてもかまわない。

【0040】次に、第 1 の送信データフォーマット変換手段 21 及び、第 N の送信データフォーマット変換手段 23 は暗号化送信データを通信路のデータフォーマット形式の第 1 の同期送信データ及び第 N の同期送信データに変換し、通信路暗号化手段 5 へ出力する。ここで、同期送信データは、例えば IEEE 1394-1995 で規定されたアイソクロナスパケットの形式のものである。

【0041】通信路暗号化手段 5 ではこれらの同期送信データを、送信認証手段 2 が出力する通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段 6 へ出力する。データ多重手段 6 は、例えば IEEE 1394-1995 に規定された方法を用いて、非同期送信

データはアシンクロナスパケットとして、暗号化同期送信データはアイソクロナスパケットとして多重化する。

【0042】送信手段7は通信路8のバスアービトレーションを行い、バスの使用权を獲得し、アシンクロナスパケットを送信先に転送するとともに、アイソクロナスパケットに対しては、例えばIEEE1394-1995プロトコルに則り、ある時間周期で周期的に送信先へ送信する。次に、ネットワーク上からデータを受信する場合、受信手段9は通信路8より自分宛のアシンクロナスパケット及びアイソクロナスパケットを受信し、データ分離手段10で多重化されたデータを分離し、アシンクロナスパケットから非同期受信データを、アイソクロナスパケットから暗号化同期受信データを取得する。

【0043】受信認証手段11は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段13へ、送信データ用の秘密キーをデータ用受信キーとしてデータ復号化手段15へ出力する。さらに、受信された制御情報は受信コマンド処理手段12で処理され、本装置内部で有効なコマンドを生成する。ここで、通信用受信キー及びデータ用受信キーは必ずしも秘密キーである必要はなく、送信認証手段2の説明で述べたのと同様の方法を用いることが可能である。

【0044】一方、通信路復号化手段13は受信認証手段11から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。第1の受信データフォーマット変換手段31及び第Nの受信データフォーマット変換手段33は同期受信データのフォーマット変換を行い、各々第1の暗号化受信データ及び第Nの暗号化受信データを生成する。ここで、例えば、第1の暗号化受信データはDVデータ形式のデータを暗号化したものであり、第Nの暗号化受信データはMPEGデータ形式のデータを暗号化したものである。また、同期送信データは、例えばIEEE1394-1995で規定されたアイソクロナスパケットの形式のものである。

【0045】第1のデータ復号化手段30及び第Nのデータ復号化手段32は、暗号化受信データを各々第1のデータ用受信キー及び第Nのデータ用受信キーで復号し、第1の受信データ及び第Nの受信データを生成する。例えば、第1の受信データはDVデータであり、第Nの受信データはMPEGデータである。これらの受信データを所望の時間間隔でDVエンコーダ及びMPEGエンコーダへ各々入力することにより映像データを得られ、例えばモニター画面上に表示することが可能となる。ここで、映像データをノンインターレス方式のプログレッシブ画像データとしてもよく、この時パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現でき

る。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【0046】以上のように本実施の形態のよれば、複数のデータ暗号化手段と複数の送信フォーマット変換手段と通信路暗号化手段を用いることにより、ストリームデータに応じた暗号化を行うことができ、例えば、DV形式で圧縮された映像データやMPEG形式で圧縮された映像データに対して、各々適切な暗号化を行える。よって、映像情報に対して必要とされる隠匿性を、各々の映像データの圧縮形式で適切な方法で暗号化でき、暗号化が容易となる。例えば、ネットワーク上にあり、通信用受信キーはあるが、データ用受信キーを持たない機器でも、見にくいが何の映像であるかは大体理解できるような映像を画像の圧縮形式に依存せず簡単に暗号化することが可能となる。

【0047】なお、本実施の形態では複数の送信データフォーマット変換手段はデータ多重化手段に接続されているとしたが、複数の送信データフォーマット変換手段をスイッチで切り替え、このうち一つを選択して、データ多重手段に接続しても良く、スイッチの切り替えを送信コマンド処理手段や送信認証手段で制御する必要があるが同様の効果が得られる。これは、複数の受信データフォーマット変換手段に対しても同様である。

【0048】また、本実施の形態では第1のデータ暗号化手段等からなるデータ送信部と第1のデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、各々の送受信データに対してデータ用送信キー及びデータ用受信キーをあらかじめ設定しておけば、例えば、映像の再生専用機器においては送信コマンド処理手段、送信認証手段、第1のデータ暗号化手段、第Nのデータ暗号化手段、第1の送信データフォーマット変換手段、第Nの送信データフォーマット変換手段、通信路暗号化手段、データ多重化手段、送信手段からなるデータ送信部のみを用いればよく、また、モニタのように映像データの受信のみを行う機器では受信コマンド処理手段、受信認証手段、第1のデータ復号化手段、第Nのデータ復号化手段、第1の受信データフォーマット変換手段、第Nの受信データフォーマット変換手段、通信路復号化手段、データ分離化手段、受信手段からなるデータ受信部のみを用いればよい。

【0049】そして、本実施の形態で示した各手段は送信手段及び受信手段の通信路ドライブ回路等を除きソフトウェアで実現しても同様の効果が得られる。また、データ多重手段及び送信手段は一つの手段で構成しても良く、同様の効果が得られる。これはデータ分離手段及び受信手段に関しても同様である。さらに、本実施の形態においても図2で示したのと同様に、送信コマンド処理

手段1と受信コマンド処理手段12を送受信コマンド処理手段16で、送信認証手段2と受信認証手段11を送受信コマンド処理手段17で実現することも可能であり、例えば、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いて暗号化することや、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いて暗号化することも容易になる。

【0050】ここでは第1のデータ暗号化手段等からなるデータ送信部と第1のデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、例えば、映像の再生専用機器においては図3と同様にして、送受信コマンド処理手段16、送受信認証手段17、第1のデータ暗号化手段20、第Nのデータ暗号化手段22、第1の送信データフォーマット変換手段21、第Nの送信データフォーマット変換手段23、通信路暗号化手段15、データ多重化手段6、送信手段7からなるデータ送信部と送受信認証手段17に接続された非同期データ用の受信手段9のみを用いて暗号化装置を構成すればよい。また、モニタのように映像データの受信のみを行う機器では図4と同様にして、送受信コマンド処理手段16、送受信認証手段17、第1のデータ復号化手段30、第Nのデータ復号化手段32、第1の受信データフォーマット変換手段31、第Nの受信データフォーマット変換手段33、通信路復号化手段13、データ分離化手段10、受信手段9からなるデータ受信部と送受信認証手段17に接続された非同期データ用の送信手段7のみを用いて復号化装置を構成すればよい。

【0051】また、本実施の形態においても図5で示したのと同様に、データ用送信キーを同期送信データとともに送信し、データ用受信キーを同期受信データとともに受信することも可能であり、データ用受信キーの取り扱いを容易にでき、通信路の秘密性を確保しつつ送受信データに対して適切な暗号化を簡単な構成で実現できる。

【0052】

【発明の効果】以上のように本発明によれば、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号化手段とを具備するこ

とにより、送受信データの内容や種類に応じた暗号化を行うことができ、隠匿性の高い送受信データに対しては強い暗号化を行うことが容易となる。

【0053】また、データ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、各々のデータ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号化手段とを具備することにより、各種の送受信データに各々応じた暗号化を行うことができ、複数の送受信データに対して柔軟に暗号化強度を変更できる。

【0054】そして、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用いて前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号化手段とを具備し、送信データ及び受信データは映像データ又は音声データ等のAVデータであることにより、各々のAVデータに対して必要とされる隠匿性を、各々の映像データの圧縮形式等に対して適切な方法で暗号化でき、暗号化が容易となる。よって、ネットワーク上にあり、通信用受信キーはあるが、データ用受信キーを持たない機器でも、見にくいが何の映像であるかは大体理解できるような映像を画像の圧縮形式に応じて簡単に暗号化することが可能となる。また、TV放送等からVTR等に録画したAVデータに対して、VTR等で再生する際に暗号化することが可能になり、著作権の保護や課金等を行うことができる。

【0055】さらに、映像データをノンインターレース方式のプログレッシブ画像データとすることにより、パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現できる。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加

工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【0056】また、データ用送信キー及び受信キーを暗号化送信データ及び暗号化受信データの一部として送受信し、通信用送信キー及び通信用受信キーを用いて通信路の暗号化を行うことにより、通信路の安全性を確保した上で、各々の送受信データに対して適切な暗号化を容易に行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態1における暗号化復号化装置のブロック図

【図2】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図3】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図4】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図5】同暗号化復号化装置におけるデータ用受信キーを同期データと共に送受信した場合のブロック図

* 【図6】本発明の実施の形態2における暗号化復号化装置の暗号化部のブロック図

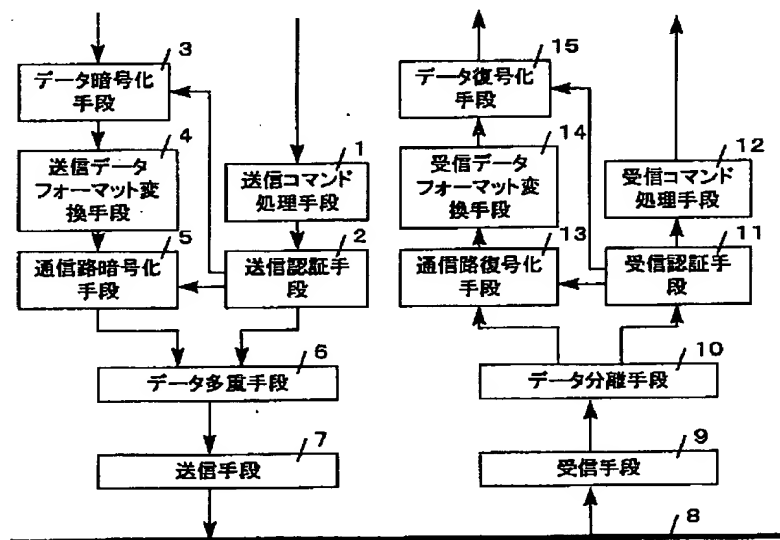
【図7】同暗号化復号化装置の復号化部のブロック図

【図8】従来の暗号化復号化装置のブロック図

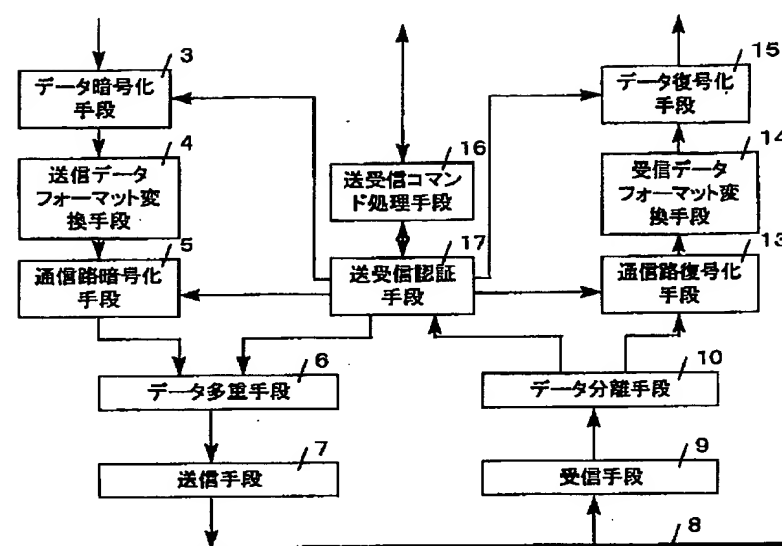
【符号の説明】

- | | |
|----|-----------------|
| 1 | 送信コマンド処理手段 |
| 2 | 送信認証手段 |
| 3 | データ暗号化手段 |
| 4 | 送信データフォーマット変換手段 |
| 5 | 通信路暗号化手段 |
| 6 | データ多重化手段 |
| 7 | 送信手段 |
| 8 | 伝送路 |
| 9 | 受信手段 |
| 10 | データ分離手段 |
| 11 | 受信認証手段 |
| 12 | 受信コマンド処理手段 |
| 13 | 通信路復号化手段 |
| 14 | 受信データフォーマット変換手段 |
| 15 | データ復号化手段 |

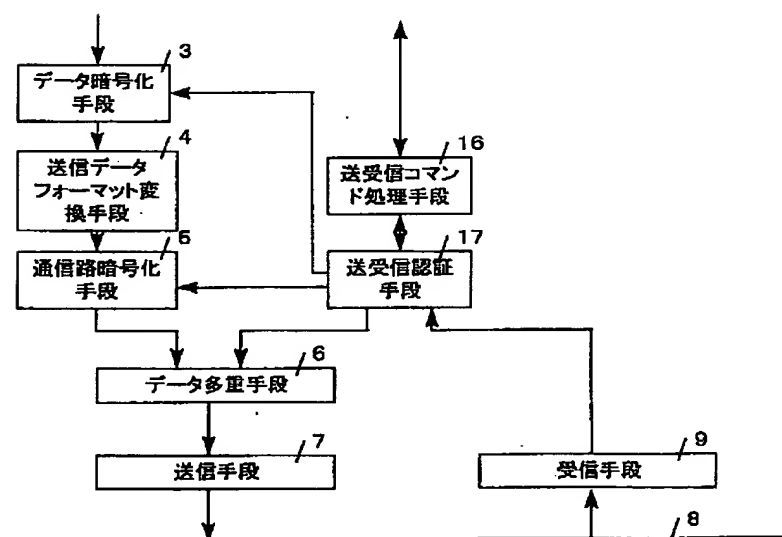
【図1】



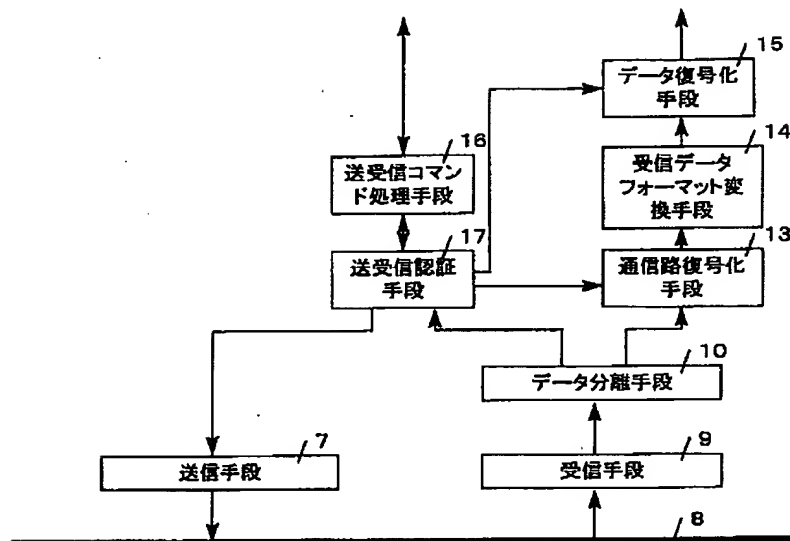
【図2】



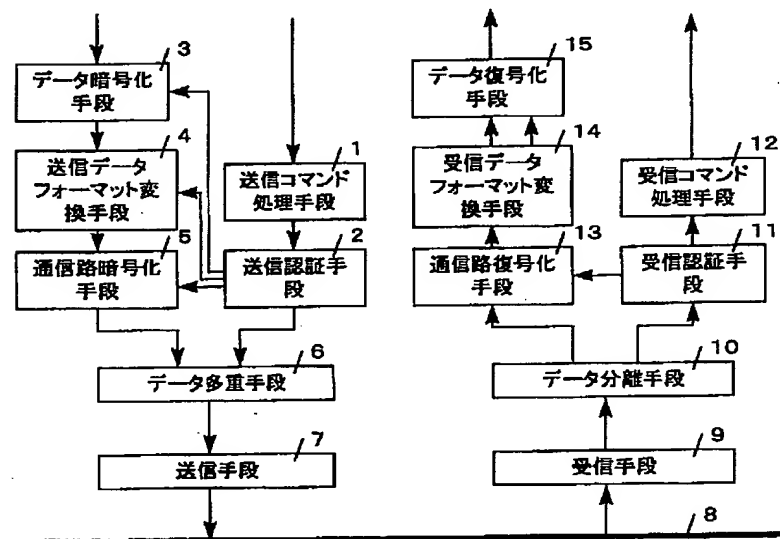
【図3】



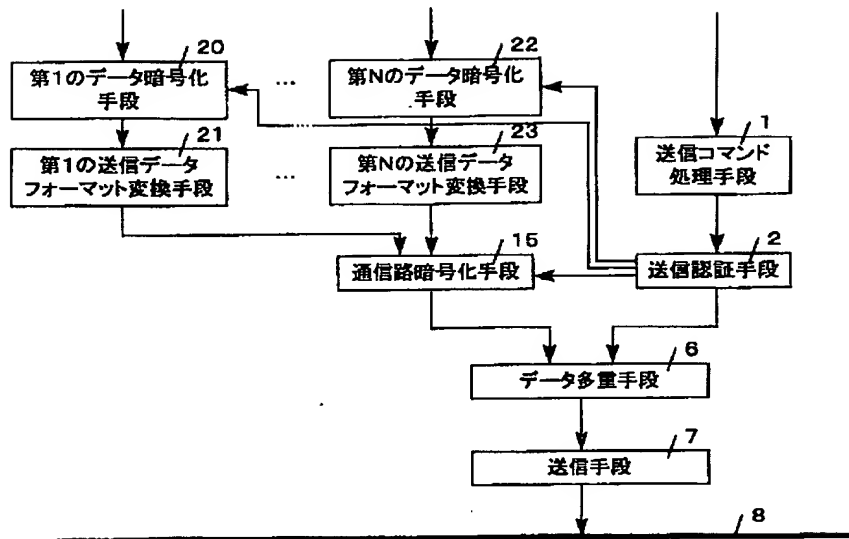
【図4】



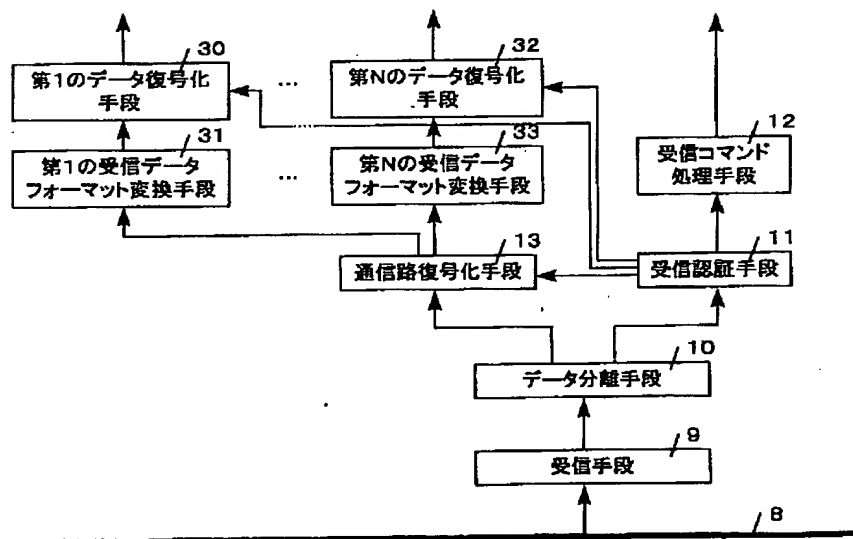
【図5】



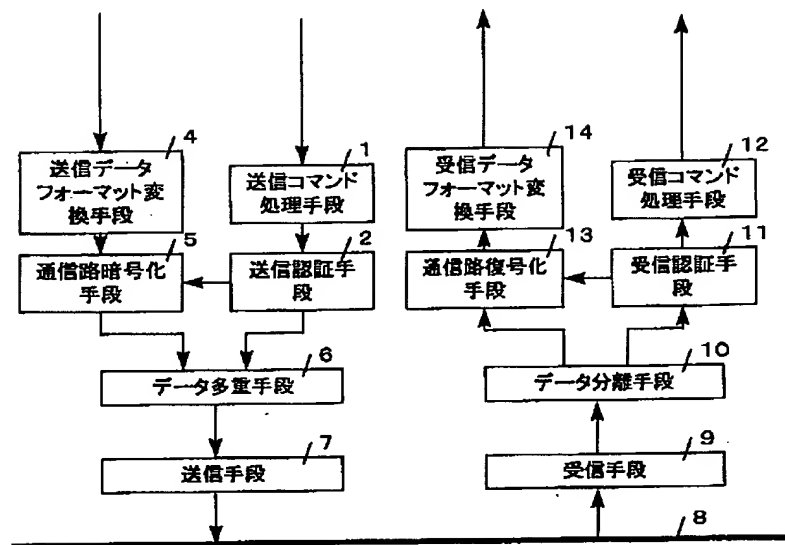
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 小林 正明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 長岡 良富
大阪府門真市大字門真1006番地 松下電器
産業株式会社内